Global Journal of Politics and Law Research, 13 (3), 48-66, 2025
ISSN: ISSN 2053-6321(Print),
ISSN: ISSN 2053-6593(Online)
Website: https://www.eajournals.org/
Publication of the European Centre for Research Training and Development–UK

Addressing AI-Driven Cyber-Terrorism Within the Framework of International Law

Mohammad Manoochehri

doi: https://doi.org/10.37745/gjplr.2013/vol13n34866 Published July 10, 2025

Citation: Manoochehri M. (2025) Addressing AI-Driven Cyber-Terrorism Within the Framework of International Law, *Global Journal of Politics and Law Research*, 13 (3), 48-66

Abstract: *AI has introduced new dimensions to cyberterrorism, enabling more sophisticated, automated, and potentially devastating attacks on critical infrastructure, democratic institutions, and global security. AI-driven tools, such as autonomous malware, intelligent surveillance systems, and deepfake technologies, have allowed terrorists to carry out complex operations with minimal human involvement and reduced detection risk. Despite these growing threats, existing international legal frameworks, such as the UN Charter [1], the Budapest Convention [2] on Cybercrime, and Security Council Resolution 1373 (2001), fail adequately to address the specific risks posed by AI-enabled cyberterrorism. The purpose of this paper is to explore the legal gaps and practical challenges associated with applying current international law to this evolving threat. A binding international treaty should be developed to define and criminalise AI-driven cyberterrorism, mandate state cooperation, and establish clear standards for prevention, attribution, and coordinated response. As a result of aligning international legal norms with emerging technological realities, the global community will be able to respond more effectively to AI-enhanced cyberthreats and build a safer, more secure digital future.*

Keywords: artificial intelligence, cyberterrorism, international law, cybersecurity policy, global governance

INTRODUCTION

The rise of AI-driven cyberterrorism poses a transformative threat to global security. Using artificial intelligence technologies, terrorist actors can automate cyberattacks, exploit vulnerabilities at scale, and spread disinformation with unprecedented efficiency. Consequently, critical infrastructure, national security systems, and public trust are increasingly at risk. In contrast to conventional cybercrime or terrorism, AI-driven cyberterrorism blurs the lines between civil, military, and autonomous operations. This risk is exacerbated by the absence of a universal definition of cyberterrorism, particularly in its AI-enhanced form. A comprehensive, binding international framework is argued for in this paper as a solution to the inadequacy of current legal instruments to address this evolving threat.

Define AI-driven cyberterrorism and its potential threats

There is a lack of scholarship on the intersection of artificial intelligence (AI), cyberterrorism, and international law. The UN Charter [3] and the Budapest Convention [4] have been widely discussed about cyberterrorism, but few studies have examined how AI-driven threats specifically challenge these legal

frameworks. In cases involving non-state actors and autonomous cyber operations, legal scholars such as Deeks and Hollis have questioned the adequacy of current attribution standards under international law. These concerns highlight how AI systems complicate accountability because they may operate independently and obfuscate the source of attacks. Additionally, the dual-use nature of AI technologies-where legitimate tools can be weaponised, raises significant regulatory and ethical concerns. The Tallinn Manual[5] and reports by Brundage et al. highlight these risks, but current international law lacks binding norms addressing them.

Despite the growing role of artificial intelligence (AI) in cyber operations, the literature also identifies a critical legal gap. A new international legal framework addressing AI-driven cyberterrorism with clear definitions, attribution standards, and enforcement mechanisms is urgently needed. AI-driven cyberterrorism involves the use of artificial intelligence (AI) technologies for political, religious, or ideological purposes to plan, execute, or amplify actions intended to cause fear, disruption, or harm through cyber means.[1] The concept of AI-driven cyberterrorism refers to the use of artificial intelligence (AI) and machine learning algorithms to carry out malicious activities, thereby enabling attackers to conduct more sophisticated, targeted, and difficult-to-detect attacks. Depending on the data they collect from their victims, these attacks can take various forms, including phishing, malware, ransomware, or social engineering techniques. AI-driven cyberterrorism refers to the use of artificial intelligence technologies by terrorist groups or malicious actors to conduct cyberattacks to inflict widespread fear, disruption, or damage. A new threat is emerging that combines the capabilities of artificial intelligence with the goals of terrorism in the digital sphere.[2]

Without a universal definition of terrorism and cyberterrorism, AI-driven cyberterrorism will be more difficult to define. A comprehensive and cohesive approach to combating AI-driven cyberterrorism requires collaboration among states. Together, states can share intelligence, resources, and best practices to strengthen their defences against such threats. As a result of this collective effort, standardised regulations and guidelines will be developed, ensuring a unified global response to cyberterrorism. For instance, AI-powered malware could dynamically evolve to avoid detection, spread more rapidly, or cause significant damage to infected systems. As a result, it is more difficult to detect and mitigate cyberattacks.

AI presents new challenges in combating cyberterrorism and offers powerful defence tools when properly deployed. Staying ahead of this evolving threat landscape will require a proactive, adaptive approach such as using AI algorithms and machine learning to enhance, automate, or accelerate cyberattacks on critical infrastructure, government systems, or civilian populations. AI's ability to operate at speed and scale offers the potential for large-scale impacts due to its ability to cause terror, panic, or disruption in society.Artificial intelligence can develop highly convincing deepfakes[3], chatbots[4], and personalised phishing attacks to manipulate individuals and spread disinformation on a large scale. As a result, terrorists may be able to recruit more supporters, raise funds, and incite violence.[5] Using artificial intelligence, terrorist groups might be able to create more sophisticated and resilient botnets capable of launching massive attacks. In addition

[1] Reza Montasari, 'Countering Cyberterrorism: The Confluence of Artificial Intelligence, Cyber Forensics, and Digital Policing' (2024) Springer.
[2] Richard Bingley, 'Combatting Cyber Terrorism – A Guide to Understanding the Cyber Threat Landscape and Incident Response Planning'(2024) IT Governance Publishing.
[3] A deepfake is a type of artificial intelligence-generated synthetic media that manipulates or replaces existing images, videos, or audio recordings to create highly convincing fake content.
[4] An AI-driven cyberattack, also known as an AI-enabled or offensive AI attack, leverages artificial intelligence and machine learning algorithms to carry out malicious activities.
[5] www.terranovasecurity.com/blog/ai-in-cyber-security

to enhancing botnet capabilities, artificial intelligence can optimise the coordination and efficiency of the network, making it more difficult to detect and dismantle.

It is possible to utilise machine learning algorithms to adapt security measures in real time, enabling the botnet to evolve continuously and evade detection. Furthermore, AI can automate the process of identifying and exploiting vulnerabilities in target systems, increasing the scale and impact of attacks. The point of the weaponisation of the internet, the role played by artificial intelligence, and the use of non-state organisations such as terrorist groups and cyberterrorism have increased.[6] However, international law will provide a reasonable and active legal framework for countering the weaponisation of the internet by AI. Increasingly sophisticated autonomous cyber weapons that can launch attacks without human intervention may emerge as AI technology advances. These tools can be programmed to adapt and evolve, making them harder to detect and neutralise. [7]

In addition, the integration of AI with the Internet of Things (IoT) may lead to attacks on interconnected devices, which would further expand the scope and impact of cyberterrorism. A terrorist could exploit AI to control large numbers of IoT devices and coordinate massive DDoS attacks or physical sabotage of critical infrastructure.[8] Moreover, AI algorithms could identify exploitable weaknesses in networks and systems faster than human hackers. Terrorists may be able to access sensitive data and critical infrastructure more easily because of this.

This is one of the most significant aspects of identifying an attacker in a cyberattack. Due to the borderless nature of the internet and the difficulty of attributing attacks to specific actors, international law faces significant challenges in addressing AI-driven cyberterrorism.[9] As a result of the anonymity provided by cyberspace, it is difficult to identify perpetrators, making it difficult to hold them accountable under international law. Moreover, the rapid evolution of technology often outpaces the development of laws and regulations, which leads to a lack of enforcement and a lack of cooperation among states.

States demand the establishment of a strong and enforceable legal framework. Artificial intelligence is being combined with malicious cyber activities to create more sophisticated and potentially devastating attacks. AI-driven cyberterrorism poses the following major threats: AI could be utilised to identify and exploit vulnerabilities in power grids, water systems, transportation networks, and other critical infrastructure.[10] The result could be widespread disruptions and potentially life-threatening situations. A machine learning algorithm may assist terrorists in predicting optimum times and targets for attacks by analysing patterns and vulnerabilities. Several potential threats associated with AI-driven cyberterrorism have been identified by the United Nations, including the fact that Artificial intelligence can automate and enhance traditional cyberattacks, making them more effective and more challenging to defend. As AI becomes more

[6] Chiheb Chebbi, 'Mastering Machine Learning for Penetration Testing' (2018) Packt ISBN: 9781788997409 www.packtpub.com/en-gb/product/mastering-machine-learning-for-penetration-testing-9781788997409/chapter/introduction-to-machine-learning-in-pentesting-1/section/artificial-intelligence-and-machine-learning-ch01lvl1sec03 accessed 10 November 2024.
[7] UNIDIR (United Nations Institute for Disarmament Research), 'Autonomous Weapon Systems and Cyber Operations' (2024) unidir.org/files/publication/pdfs/autonomous-weapon-systems-and-cyber-operations-en-690.pdf accessed 10 November 2024.
[8] Lucia Stanham, 'AI-Powered Cyberattacks' (2025) www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/ai-powered-cyberattacks/ Accessed 11 November 2024.
[9] Tripti Bhushan, 'Artificial Intelligence, Cyberspace and International Law' 2024 21(2) O.P. Jindal Global Law School scholarhub.ui.ac.id/cgi/viewcontent.cgi?article=1745&context=ijil accessed 13 November 2024.
[10] Kolawole Samuel Adebayo, 'The Answer To AI-Driven Attacks On Critical Infrastructure: Resiliency' (2025) Forbes www.forbes.com/sites/kolawolesamueladebayo/2025/03/25/the-answer-to-ai-driven-attacks-on-critical-infrastructure-resiliency/ accessed 18 November 2024.

widespread, it will reduce the skills and technical expertise needed to use it for malicious purposes, potentially enabling more terrorist groups to take advantage of it.[11] Another threat is disinformation campaigns. Terrorists may use artificial intelligence to generate and spread convincing false information, deepfakes, and propaganda on a large scale. It could be used to manipulate public opinion, incite violence, or undermine trust in institutions.[12]

One of Al's new threats is targeted Phishing and Social Engineering. AI is used to enhance phishing techniques by analysing vast amounts of data to create highly personalised and convincing messages tailored to the individual recipient. The software can mimic familiar writing styles or use information from social media profiles to craft emails that appear to come from trusted sources.[13] The sophistication of phishing attacks increases the likelihood that victims will provide sensitive information, such as passwords or financial information, unknowingly. The chances of successfully manipulating individuals into disclosing sensitive information have increased as a result.

There is also a threat that Al can pose through terrorist organisations. It is possible that AI-driven autonomous weapons could be programmed to select and engage targets without human intervention, resulting in unpredictable and uncontrollable outcomes.[14] A terrorist organisation may be able to hack or misuse these weapons to carry out attacks with precision and efficiency, resulting in significant casualties and destruction. In the hands of malicious actors, autonomous weapons pose a particularly dangerous threat due to their lack of accountability and potential for rapid escalation in conflicts.

Highlight the difficulties in applying existing international law to this emerging phenomenon.
International law applies to emerging phenomena, such as advanced technologies, cyber warfare, artificial intelligence, or environmental challenges, which pose significant challenges. Generally, existing international laws, such as the UN Charter[6] or the Geneva Conventions, lack specific provisions to address new issues. International law often relies on interpretations and adaptations of existing frameworks to address these evolving challenges. However, concepts such as cyber-attacks, autonomous weapons, or AI decision-making do not have universally agreed-upon definitions in international law, which creates ambiguity. Moreover, fostering cooperation between states through bilateral or multilateral agreements can assist in creating a unified understanding and facilitate the adoption of universally accepted definitions.
Technology or circumstances may have already outgrown new treaties by the time they are developed. There is a need for legal scholars and even policymakers to provide a better solution to this problem. A major role played by technology is that it continuously introduces new challenges and opportunities that

[11] UNCCT and UNICRI (Cyber Security and New Technologies Unit of the United Nations Counter-Terrorism Centre in the United Nations Office of Counter-Terrorism and the United Nations Interregional Crime and Justice Research Institute, 'Algorithms and Terrorism: The Malicious Use of Artificial Intelligence for Terrorist Purposes' (2021), unicri.it/sites/default/files/2021-06/Malicious%20Use%20of%20AI%20-%20UNCCT-UNICRI%20Report_Web.pdf accessed 12 November 2024.
[12] Sangfor Technologies, 'Defining AI Hacking: The Rise of AI Cyber Attacks' (2024) www.sangfor.com/blog/cybersecurity/defining-ai-hacking-rise-ai-cyber-attacks accessed 20 November 2024.
[13] Mailgun Blog, 'The golden age of scammers: AI-powered phishing' (2024) <www.mailgun.com/blog/email/ai-phishing/> accessed 22 November 2024.

[14] Alexander Blanchard and Jonathan Hall KC, 'Terrorism and Autonomous Weapon Systems: Future Threat or Science Fiction?' (2023) Alan Turing Institute cetas.turing.ac.uk/publications/terrorism-and-autonomous-weapon-systems-future-threat-or-science-fiction accessed 5 December 2024.

must be addressed by future legal frameworks. Technology advances create novel scenarios that existing laws may not adequately cover, requiring policymakers to adopt regulations to keep pace with innovation. Additionally, technology can aid in the legislative process itself by offering tools for more efficient legal research, drafting, and enforcement.

However, many emerging technologies have both civilian and military applications, complicating their regulation under existing regulatory frameworks. The current legal system makes it difficult to determine responsibility and jurisdiction in cases of cross-border phenomena (e.g., cybercrime or environmental degradation).[15] Due to these challenges, Al in cyber-terrorism will develop alternative aspects and pose a significant problem for international law. Although many emerging issues involve non-state actors (e.g., corporations and terrorist groups), international law is traditionally a state-centric system. Alternatively, States may resist external interference, resulting in difficulty in enforcing international laws. In addition to AI-driven cyberterrorism challenges, there are other aspects to consider. The dual-use capability of these AI technologies refers to their ability to be used both for civilian purposes (e.g., healthcare, transportation, education) as well as for military or security purposes (e.g., autonomous weapons, surveillance, cyber warfare). As a result of this dual nature, governance, regulation, and the application of international law present significant challenges.
It is possible for malicious actors, including terrorist organisations and rogue states, to misuse civilian AI (e.g., autonomous weapons, cyberattacks), and it is difficult to control and regulate, leading to widespread dissemination, including to non-state actors. In addition, AI may blur the distinction between civilian and military targets, complicating compliance with IHL (International humanitarian law) principles such as distinction and proportionality. As a result of nations racing to develop military AI capabilities, there is a risk of escalating global tensions and destabilising international security.[16]

Therefore, AI systems can behave unpredictably or cause unintended harm, particularly when used autonomously in critical situations, which is one of the most potent threats posed by AI. AI systems can behave unpredictably or cause unintended harm, particularly when used autonomously in critical situations, which is one of the most potent threats posed by AI.[17] However, economic inequalities and regulatory gaps regarding AI-driven cyberterrorism may be irrefutable points regarding the new issue in international law. Inequalities in access to dual-use AI technologies can exacerbate global inequalities between developed and developing states, and the existing international frameworks are unable to address the unique challenges presented by AI's dual-use nature, leaving gaps in accountability and governance.

1.3. Emphasise the need for a comprehensive legal framework to address AI-driven cyberterrorism.

AI-driven cyberterrorism poses unprecedented challenges that existing legal frameworks cannot address. A comprehensive legal framework is necessary in light of the rapid development of artificial intelligence and its potential for misuse. The UN Charter[7], the Geneva Conventions, and the Budapest Convention[8] on Cybercrime do not address the role of AI in cyberterrorism. It is therefore imperative that governments develop new legislation to address the new challenges posed by artificial intelligence and cyberterrorism. Measures should be taken to prevent and prosecute malicious use of artificial intelligence, as well as to

[15] Kelley M. Sayler , 'Emerging Military Technologies: Background and Issues for Congress' (2024) Congressional Research Service (R46458) sgp.fas.org/crs/natsec/R46458.pdf accessed 10 December 2024.
[16] Carlos Batallas, 'When AI Meets the Laws of War' (2024) IE University www.ie.edu/insights/articles/when-ai-meets-the-laws-of-war/#:~:text=By%20maintaining%20human%20oversight%2C%20addressing,upholding%20the%20rule%20of%20law. accessed 12 December 2024.
[17] Roman V. Yampolskiy , 'AI Unexplainable, Unpredictable, Uncontrollable' (2024) Taylor & Francis Group www.taylorfrancis.com/books/mono/10.1201/9781003440260/ai-roman-yampolskiy accessed 14 December 2024.

safeguard and protect data. It is necessary to establish a unified legal definition of AI-driven cyberterrorism to distinguish between criminal, state-sponsored, and terrorist activities. In order to prevent misuse and promote accountability, ethical and responsible standards must be established for using artificial intelligence in cyberspace.

Artificial intelligence systems are capable of executing cyberattacks independently without the intervention of humans. As a result, there are legal ambiguities regarding accountability and intent. The regulation of AI-driven cyberattacks presents challenges since traditional legal frameworks are not designed to deal with autonomous decision-making. When an AI system acts independently, assigning liability is difficult, and determining intent is complicated by the absence of human involvement. Moreover, advances in artificial intelligence technology are outpacing the development of corresponding legal and regulatory frameworks.[18] AI-driven attacks can exploit vulnerabilities across interconnected systems, causing widespread disruptions to critical infrastructure, financial systems, and national security. As AI and cyber capabilities advance rapidly, existing laws are unable to keep up, leaving gaps in addressing new threats.[19] There is one important point related to AI that needs to be discussed, and this is similar to the role that non-state organisations play in cyberterrorism.

In order to emphasise the need for a comprehensive legal framework for AI-driven cyberterrorism, it is necessary first to understand the definition of terrorism and cyberterrorism in the current era and, secondly, to offer a new perspective on AI-driven cyberterrorism. In this new framework, AI-driven cyberterrorism should be defined clearly and distinguished from traditional cyber threats. Guidelines should be established for international cooperation in intelligence sharing and joint response strategies. Furthermore, the framework must outline mechanisms for accountability and sanctions against state and non-state actors who support or engage in AI-driven cyberterrorism.

A proactive legal approach is necessary to address the potential misuse of AI in cyberterrorism. By creating a comprehensive framework, gaps in existing laws will be bridged, international cooperation will be fostered, accountability will be enhanced, and global security will be protected. Establishing such a framework is imperative to mitigate the risks posed by AI-driven cyber threats while safeguarding innovation and human rights.

Attribution Challenges

Discuss the issue of attribution in cyberattacks, which is further complicated by the use of AI systems. Since cyberattacks are inherently anonymous, transnational, and rely on obfuscation techniques, attribution of the responsible party has always been difficult. AI has significantly exacerbated these problems by adding layers of complexity and unpredictability to cyberattacks.[20] Introducing AI into existing legal frameworks requires a comprehensive understanding of rapidly evolving technologies and their implications. In order to address the complexity of AI behaviour, lawmakers must grapple with the fact that it is unpredictable

[18] Pagallo, U, 'The Laws of Robots: Crimes, Contracts, and Torts.' (2013) Springer / Cath, C., et al. 'Artificial Intelligence and the 'Good Society': The US, EU, and UK Approach' (2018) 24(2) Science and Engineering Ethics, 505–528.
[19] Singer, P. W., & Friedman, A. 'Cybersecurity and Cyberwar: What Everyone Needs to Know.'(2014) Oxford University Press / Brundage, M., et al. 'The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation' (2018) arXiv arxiv.org/abs/1802.07228 accessed 7 January 2025.
[20] Lorraine Finlay and Christian Payne, 'The Attribution Problem and Cyber Armed Attacks' 2019 113 Cambridge University Press www.cambridge.org/core/journals/american-journal-of-international-law/article/attribution-problem-and-cyber-armed-attacks/ADC0F451A9B560D8A070A753E61E874F accessed 5 January 2025.

and difficult to attribute to a single actor. A balance must also be struck between innovation and regulation, ensuring that new laws do not stifle technological advancement while still protecting against potential threats.[21]

To conceal their identities, cybercriminals often use techniques such as IP spoofing, encryption, and proxy servers. In addition to steganography, cybercriminals also employ polymorphic malware, which constantly changes its code to avoid detection by security software. Furthermore, they use dark web marketplaces to trade tools and information, complicating efforts to track and dismantle their operations. Al contributes to this process. In order to conceal their tracks, AI systems may employ advanced techniques such as dynamically changing IP addresses or encrypting communication pathways. It is common for attackers to execute attacks using third-party actors or compromised systems (e.g., botnets), obscuring their involvement even further.[22]

In addition, state and non-state actors frequently use intermediaries to execute cyberattacks, which makes direct attribution difficult. This is one of the main reasons that Al will be able to provide an easier method of developing or stopping it. An AI-driven solution may involve the development of advanced threat detection systems that use machine learning to detect suspicious patterns and anomalies in real time.[23]

In addressing cyber terrorism, the impact of artificial intelligence on attribution is examined. AI systems can act autonomously once programmed, blurring the lines of accountability. A computer program might, for example, adapt its attack strategy based on real-time conditions, making it difficult to trace the source of its actions. If an AI system executes an attack without direct human intervention, it is unclear whether the programmer, the user, or the organisation deploying the AI is responsible for the action.[24]

The majority of artificial intelligence tools are dual-purpose, meaning that they can be used for both legitimate and malicious purposes. It is therefore difficult to determine whether a system was deployed intentionally to commit an attack. There is the possibility that AI systems may behave unintentionally as a result of programming errors or unforeseen interactions, raising the question of whether an attack was deliberate or unintentional.[25]

The other point will be the legal and ethical implications. According to international law, states are responsible for cyber operations conducted by their agents. It is difficult, however, to prove state involvement in AI-driven cyberattacks, especially if proxies or autonomous systems are used. In this scenario, encourage developers to adhere to ethical guidelines when designing and deploying AI systems, thereby reducing the risk of misuse.[26]

[21] UNIDIR (United Nations Institute for Disarmament Research) 'AI and Cybersecurity Workshop: The Challenges of New and Updated Threats' (2024) unidir.org/event/ai-and-cybersecurity-workshop-the-challenges-of-new-and-updated-threats/ accessed 10 January 2025.
[22] Cath, C., et al. "Artificial Intelligence and the 'Good Society': The US, EU, and UK Approach." (2018) 24 Springer, 505–528. link.springer.com/article/10.1007/s11948-017-9901-7 accessed 11 January 2025.
[23] CYBLE, 'Harnessing the Power of AI for Real-Time Threat Detection' (2024) cyble.com/knowledge-hub/real-time-threat-detection-with-ai/#elementor-toc__heading-anchor-0 accessed 12 January 2025.
[24] Bryson, J. J., Diamantis, M. E., & Grant, T. D. "Of, For, and By the People: The Legal Lacuna of Synthetic Persons." Artificial Intelligence and Law, 2017 25(3), 273–291. link.springer.com/article/10.1007/s10506-017-9214-9 accessed 13 January 2025.
[25] Nick Bostrom, 'Superintelligence Paths, Dangers, Strategies' (2017) Oxford University Press.
[26] Schmitt, M. N. (Ed.) Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.(2017) Cambridge University Press./UNGGE ((United Nations Group of Governmental Experts on Information Security), 'Report on Developments in the Field of Information and Telecommunications in the Context of International Security.(2015)./UNESCO (United Nations Educational, Scientific and Cultural Organisation) 'Recommendation on the Ethics of Artificial Intelligence (2023) unesdoc.unesco.org/ark:/48223/pf0000381137 accessed 14 January 2025.

It is possible to train these systems to recognise sophisticated attack vectors that traditional methods might not be able to recognise. Additionally, artificial intelligence can be used to automate the response to cyber threats, allowing for faster containment and mitigation of damage before it spreads. However, the Regulation of this process would present a significant challenge. One of the greatest challenges is ensuring that these AI-driven systems do not inadvertently violate privacy rights while monitoring for threats. Furthermore, the issue of establishing accountability for AI actions, particularly in autonomous decision-making scenarios, presents a complex dilemma. The evolving landscape will require ongoing adjustments to regulatory frameworks to strike a balance between innovation and security, as well as privacy concerns.[27] Thus, investigating AI-driven cyberattacks often requires intrusive measures, raising ethical considerations related to the balance between privacy rights and security requirements

Challenges of Attribution in AI-Driven Cyberterrorism: Implications for State Responsibility and the Role of International Cooperation

The ability of artificial intelligence (AI) to execute cyberattacks autonomously, adapt its strategies, and obfuscate its origins makes attribution increasingly difficult. An attribution process is essential for enforcing state responsibility under international law, however, AI-driven cyber operations are anonymous, decentralised, and transnational.[28] Through enhanced international cooperation and information sharing, this article explores how the lack of clear attribution hinders the application of international law principles, particularly state responsibility.

According to international law, states are responsible for cyber operations conducted by their agents. However, AI-driven cyberterrorism poses significant legal challenges. The AI-driven nature of cyberterrorism makes it difficult to determine who is responsible for an attack, as AI systems can be programmed to act without human intervention.[29] As a result, it is difficult to determine whether a state is legally responsible. Furthermore, AI-driven cyberterrorism can evade traditional international laws, making it even more difficult to hold states accountable.

Another important aspect of AI is that existing laws, such as the UN Charter[9] on State Responsibility, were not designed for autonomous, AI-driven cyber operations, creating enforcement gaps. Furthermore, defining intent in AI-driven cyberattacks is a challenging task, which further complicates legal attribution. Artificial intelligence has the potential to enhance as well as disrupt existing cybersecurity frameworks. In one sense, artificial intelligence can enhance the detection and response to threats by analysing large quantities of data in order to detect vulnerabilities and suspicious activity. In contrast, the integration of artificial intelligence into cyber operations introduces new complexities, including the need to adapt existing legal frameworks to address issues of intent and accountability.

Existing Legal Framework

Analyse the applicability of current international counter-terrorism conventions and UN Security Council resolutions

[27] Brundage, M., et al. 'The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation. (2018) Cornell University Arxiv arxiv.org/abs/1802.07228 accessed 12 January 2025.
[28] Fabio Cristiano, Dennis Broeders, François Delerue, Frédérick Douzet, Aude Géry, 'Artificial Intelligence and International Conflict in Cyberspace' (2023) Routledge doi.org/10.4324/9781003284093 accessed 11 January 2025.
[29] Rahul Sahu& Shivangi Tripathi. 'Legal challenge in combatting cyber terrorism'(2024) AFJBS (African Journal Biological Science) doi.org/10.33472/AFJBS.6.Si2.2024.1203-1213 accessed 25 January 2025.

The international legal framework for counterterrorism is composed of multilateral treaties, UN Security Council resolutions, and customary international law. Although these instruments are intended to prevent, criminalise, and respond to terrorist activities, their applicability can vary depending on the evolving nature of terrorism, including cyberterrorism and AI-driven threats.[30] An evaluation of the effectiveness and limitations of existing international counter-terrorism conventions and key UNSC resolutions is presented in this analysis.[31] Cyberterrorism, particularly AI-driven cyberterrorism, poses challenges to existing international counterterrorism conventions and UN Security Council (UNSC) resolutions. Although these legal frameworks were originally intended to combat traditional terrorism, their applicability to cyber-based threats- especially those involving artificial intelligence (AI)-remains uncertain.

Through the use of artificial intelligence, modern terrorism strategies have been significantly influenced by the automation of attacks and the development of sophisticated cyber weapons. By artificial intelligence, terrorists can enhance the precision and impact of their operations, such as through deepfake propaganda, which can spread misinformation and incite violence. The use of AI-driven tools can also assist terrorists in identifying vulnerable targets and optimising their tactics for maximum disruption.Artificial intelligence can be used by attackers to mask their identities, plant false flags, and rapidly modify infrastructure, making it difficult to trace the source of an attack. Proxy servers, anonymisers, and botnets further complicate the attribution process, creating a "digital fog" for investigators to navigate.[32]

International law requires that the wrongful conduct of a state be attributable to it. The complexity of AI-driven attacks, however, makes attribution difficult and prone to error.[33] A misattribution may lead to severe consequences, including the wrong accusation of innocent entities, the escalation of conflicts, and the retaliation against the wrong targets. Before claiming attribution, it is essential to conduct a thorough investigation and consider all relevant factors.

Therefore, the majority of international counter-terrorism conventions[34] Regional Conventions do not explicitly address AI-driven cyberterrorism, which requires updates to consider digital threats and AI-based threats. In order to combat AI-driven threats, it is essential to develop comprehensive international regulations that specifically address the use of artificial intelligence in terrorist activities. Governments, technology companies, and cybersecurity experts can collaborate more effectively to share intelligence and best practices to combat these sophisticated threats. Research and development of AI-based defence systems can also assist in detecting and neutralising potential attacks before they escalate. Although the UNSC has issued a number of binding resolutions regarding terrorism, many of which provide a legal basis for countering cyber threats. Despite this, there are gaps in the understanding of AI-driven cyberterrorism. This is one of the challenges that the international community has been faced with. In terms of the definition of terrorism and cyber terrorism, it is followed by AI-driven cyber terrorism. As a matter of importance, the UN has not issued any recommendations.

[30] Ana María Salinas de Frías, Katja Samuel, and Nigel White, 'Counterterrorism: International Law and Practice' (2012) Oxford University Press
[31] UN Security Council Resolutions 1373 (2001), 1540 (2004), 2178 (2014), and 2396 (2017)
[32] Clementine Swate, Siphesihle Sithungu and Khutso Lebea, *An Analysis of Cyberwarfare Attribution Techniques and Challenges* (University of Johannesburg 2006).
[33] Bérénice Boutin, 'State responsibility in relation to military applications of artificial intelligence' 2022 36(1) *Leiden Journal of International Law* www.cambridge.org/core/journals/leiden-journal-of-international-law/article/state-responsibility-in-relation-to-military-applications-of-artificial-intelligence/1B0454611EA1F11A8B03A5D2D052C2BE Accessed 2 February 2025.
[34] The 1997 International Convention for the Suppression of Terrorist Bombings, The 1999 International Convention for the Suppression of the Financing of Terrorism, The 2005 International Convention for the Suppression of Acts of Nuclear Terrorism.

The primary concern in this regard would be the lack of provisions for coordinated responses to AI-enabled attacks on critical infrastructure by the United Nations. A critical point to note is that uncoordinated responses to AI-enabled attacks can result in significant vulnerabilities in global infrastructure. Without a unified approach, individual nations may find it difficult to effectively defend against or mitigate these sophisticated threats, which may result in widespread economic damage and loss of life. Furthermore, inconsistent strategies may impede international cooperation and compromise efforts to develop resilient defence mechanisms against AI-driven cyberterrorism in all aspects, including weapon control systems, intelligence sharing on AI-enabled threats, and the finance sector.

A number of legal and operational gaps exist when it comes to addressing AI-driven cyberterrorism. As a result of these gaps, a fragmented global response may result, putting critical infrastructure at risk of AI-driven attacks. This may result in severe disruptions to essential services such as power grids, healthcare systems, and financial institutions. As states struggle to attribute attacks and hold perpetrators accountable, this disarray could foster international tensions and even conflict. A major gap in international legal instruments is the lack of an explicit definition of AI-driven cyberterrorism, which creates ambiguities in prosecution and enforcement. A legal definition of AI-driven cyberterrorism should be established under the framework of the United Nations. [35]

While current counterterrorism laws focus on human-directed actions, AI-driven cyberattacks may operate autonomously. It will be necessary to amend counter-terrorism conventions to include AI-driven autonomous threats and to define state responsibility in such situations.[36]

The role of states, many states lack the technical expertise to investigate AI-driven cyberterrorism, and intelligence sharing is inconsistent. Nevertheless, the solution will be to establish an AI-focused cyberterrorism intelligence-sharing network, like Interpol's Global Cybercrime Strategy.[37]

Systems developed for cyber defence can be repurposed for cyber offences, creating a dual-use dilemma. In order to ensure responsible AI development in cybersecurity, international law should establish ethical standards for AI development. This is the case with Al-Driven cyber terrorism. It is a new gap in international law as to how dual-use threats should be addressed.
Although current international counter-terrorism conventions and UNSC resolutions provide a partial framework for addressing AI-driven cyberterrorism, substantial gaps remain. A lack of a legal definition, insufficient provisions for AI autonomy, and insufficient international cooperation hinder effective countermeasures. As a result of updating legal frameworks, improving intelligence-sharing mechanisms,

[35] UNCCT (United Nations Counter-Terrorism Centre), *Algorithms and Terrorism: The Malicious Use of Artificial Intelligence for Terrorist Purposes* (2021) www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/malicious-use-of-ai-uncct-unicri-report-hd.pdf accessed 6 February 2025.
[36] United States (Office for Disarmament Affairs), *Background on LAWS in the Convention on Certain Conventional Weapons* (2023) disarmament.unoda.org/the-convention-on-certain-conventional-weapons/background-on-laws-in-the-ccw/?utm_source=chatgpt.com accessed 5 February 2025. / United Nations (Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems), '*Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons* Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects' (2023) https://docs-library.unoda.org/Convention_on_Certain_Conventional_Weapons_Group_of_Governmental_Experts_on_Lethal_Autonomous_Weapons_Systems_(2023)/CCW_GGE1_2023_CRP.1_0.pdf accessed 5 February 2025.
[37] Interpol, *'Cybercrime Global strategy'* (2025) www.interpol.int/Media/Documents/WPS?limit=12&page=2 accessed 5 February 2025. / Ersin Cahmutoglu, 'The threat of AI-driven cyber warfare is real and it can disrupt the world '(2025), *TRT World* www.trtworld.com/opinion/the-threat-of-ai-driven-cyber-warfare-is-real-and-it-can-disrupt-the-world-18244256 accessed 5 February 2025

and implementing ethical AI governance, the international community can better respond to the growing threat of AI-driven cyberterrorism.

Discuss the role of national legislation in addressing AI-driven cyberterrorism.
A growing threat to national and international security is AI-driven cyberterrorism, which requires robust legislative frameworks to prevent, detect, and mitigate such attacks. International agreements provide overarching principles, but national legislation plays a vital role in translating these principles into enforceable laws, establishing accountability, and ensuring effective responses. The purpose of this discussion is to examine how national legal frameworks can assist in countering AI-driven cyberterrorism, to examine existing laws, to highlight legal gaps, and to propose strategies for strengthening domestic legal frameworks.

A national legal framework serves as the first line of defence against AI-driven cyberterrorism. By establishing clear regulations on the development and use of AI technologies, national laws can mitigate AI cyber threats, ensuring that they adhere to security standards and ethical guidelines. These laws may also require robust cybersecurity measures for critical infrastructures and require organisations to regularly update and test their defences against emerging AI-driven threats. Further, national legislation can facilitate the sharing of intelligence and the development of coordinated responses to potential cyberterrorism incidents between government agencies, the private sector, and international partners.

National laws, however, define cyberterrorism offences and provide clear penalties for AI-driven cyberattacks. There are provisions in the USA PATRIOT Act (2001)[38] for prosecuting cyberterrorism, however, it does not address the threat comprehensively posed by artificial intelligence. It demands that terrorist acts be recognised as crimes. After the terrorist attacks of September 2001, this is a perspective promotion.

The rapidly evolving nature of AI technology, which constantly outpaces legislative efforts, is one of the primary challenges in defining AI-driven cyberterrorism. As a result, it is difficult to establish a clear and consistent legal definition of AI that encompasses all possible threats associated with it. Cyberterrorism offences are further complicated by the difficulty of distinguishing between malicious AI activities and legitimate AI innovations.[39]

To ensure responsible AI development and prevent misuse for cyberterrorism, regulations should make a statement about Al-driven cyber terrorism. To ensure that AI systems are resilient against attacks, possible regulatory measures could include mandatory security audits. Additionally, developers may be required to implement robust oversight mechanisms to detect and prevent unauthorized use of artificial intelligence. For example: According to the European Union's AI Act (proposed 2021), AI applications are classified according to their risk level, with cybersecurity threats being classified as high-risk AI systems.

Another point would be cyber defence and intelligence measures. National cybersecurity strategies can enable real-time monitoring and response to AI-driven cyberattacks. Other point would be cyber defence and intelligence measures. National cybersecurity strategies can enable real-time monitoring and response

[38] US Department of Justice, *What Is the USA PATRIOT Act?* www.justice.gov/archive/ll/what_is_the_patriot_act.pdf accessed 10 June 2025.
[39] European Commission, '*AI Act*' (2024) digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai accessed 6 February 2025

to AI-driven cyberattacks. For example, China's Cybersecurity Law (2017)[40] requires strict cybersecurity measures, including AI regulation. According to this law, network operators are required to implement cybersecurity measures and cooperate with authorities in matters related to national security and criminal investigations. The measures, however, are intended to enhance China's ability to monitor and respond to cyber threats, including those that could be influenced by artificial intelligence. While the law has been criticised for its potential to increase government control over information and increase security risks for businesses, it represents an important step forward in the development of a national cybersecurity strategy.[41] Using artificial intelligence tools, agencies can track, investigate, and prosecute cyberterrorists. The use of artificial intelligence plays a key role in the detection of cyber-terrorist activities by identifying patterns and anomalies in vast amounts of data. As a result of machine learning algorithms, potential threats can be detected quickly by recognising unusual behaviour that differs from the norm. By doing so, agencies can respond proactively, mitigating risks before they escalate into a significant security risk. Example: The UK National Cyber Security Centre (NCSC) provides intelligence-sharing frameworks for AI-driven threat detection.[42]

Despite efforts to regulate AI and cybersecurity, there remain several legal and operational challenges. Cyberterrorism driven by artificial intelligence is not explicitly addressed in many national counterterrorism laws. There is a lack of specific legal provisions relating to artificial intelligence.[43] Also, AI tools developed for legitimate cybersecurity purposes may be repurposed for cyberterrorist purposes, and a solution may be to introduce licensing and monitoring for AI tools with dual-use capabilities.[44]

Update laws to attribute legal responsibility for autonomous AI actions. Due to their dual-purpose nature, AI tools can be used for both beneficial and malignant purposes, posing a significant challenge to regulation and control. Due to this ambiguity, efforts to ensure that AI technologies are used responsibly are complicated, as the same algorithms that enhance cybersecurity can also be manipulated to facilitate cyberattacks. Therefore, robust frameworks are needed to monitor and regulate the development and deployment of these technologies to prevent their misuse.

Lastly, it is possible to enhance extradition treaties and legal harmonisation to prosecute cyberterrorists internationally. The main challenge is to address the challenge of cyberterrorism effectively. It is possible to hold cybercriminals accountable regardless of their location by strengthening international cooperation. As a result, this approach not only deters potential offenders but also promotes a safer and more secure global digital environment. [45]

[40] KPMG, *Overview of Cybersecurity Law* (2017) assets.kpmg.com/content/dam/kpmg/cn/pdf/en/2017/02/overview-of-cybersecurity-law.pdf accessed 10 June 2025.
[41] Osborne Clarke, Cyber Security China (2019) www.osborneclarke.com/wp-content/uploads/2019/12/China-Hong-Kong-Cybersecurity-Law-Report-December-2019.pdf accessed 6 February 2025. /Securiti, 'What Is China's Cybersecurity Law' (2024) securiti.ai/what-is-china-cybersecurity-law/ accessed 6 February 2025.
[42] Shilpa Mahajan, Mehak Khurana and Vania Vieira Estrela, *Applying Artificial Intelligence in Cybersecurity Analytics and Cyber Threat Detection* (John Wiley & Sons Inc 2024) onlinelibrary.wiley.com/doi/book/10.1002/9781394196470 accessed 10 February 2025.
[43] Plixavra Vogiatzoglou, 'The AI Act National Security Exception' (2024) VerfBlog verfassungsblog.de/the-ai-act-national-security-exception/#:~:text=10.59704/292082becc7cc8e6. accessed 10 February 2025.
[44] Lorenzo Pupillo, Stefano Fantin, Afonso Ferreira and Carolina Polito, '*Artificial Intelligence and Cybersecurity CEPS Task Force Report Technology, Governance and Policy Challenges*' (2021), Centre for European Policy Studies (CEPS)
[45] The United Nations Office on Drugs and Crime (UNDOCS) 'The Commission on Crime Prevention and Criminal Justice, 'Resolution 26/4 Strengthening international cooperation to combat cybercrime'

National legislation plays a crucial role in combating AI-driven cyberterrorism by criminalising offences, regulating AI tools, and enhancing cybersecurity enforcement. To address AI-driven cyber threats, several nations have implemented legal measures. As a consequence, gaps in AI-specific legal provisions, challenges in attributing AI attacks, and jurisdictional limitations remain significant obstacles. To effectively combat AI-driven cyberterrorism while ensuring national security and compliance with international norms, governments must strengthen legal definitions, implement AI regulations, foster global cooperation, and invest in AI forensic capabilities.

Potential Legal Developments & Recommendations

Propose the development of a new international legal instrument specifically addressing AI-driven cyberterrorism.

Artificial intelligence (AI) has created new challenges in cybersecurity, particularly in the context of cyberterrorism. Artificial intelligence-driven cyberterrorism poses several unique threats, such as autonomous cyberattacks, deepfake-enabled propaganda, AI-powered disinformation campaigns, and AI-driven malware that is capable of evading traditional detection systems. There are no explicit provisions to address these emerging threats in existing international legal frameworks, such as the Budapest Convention[10] on Cybercrime and resolutions of the UN Security Council on counterterrorism. An International Legal Instrument on AI-driven cyber terrorism is needed to establish clear guidelines and regulations for the use of AI in cybersecurity. It would be possible to ensure that AI technologies are developed and deployed responsibly, thereby preventing misuse and enhancing global cooperation in combating cyber threats.

In addition, the rapid integration of AI into cyber operations has transformed the landscape of terrorism, making it possible for autonomous, adaptive, and highly efficient cyberattacks to be conducted. Currently, available legal definitions of terrorism and cyberterrorism do not adequately address the complexities introduced by artificial intelligence driven cyber threats. Comparing AI-driven cyberterrorism with traditional cyberterrorism definitions may help develop a more effective international legal framework to address emerging AI threats.

The table (Comparison of Traditional vs AI-Driven Cyberterrorism)[46] The above illustrates the differences between cyberterrorism and AI-driven cyberterrorism. To provide a new legal framework for al-driven cyber terrorism, it will be helpful to have a better understanding of it. In this regard, defining terrorism and cyber terrorism as aspects of terrorism will be beneficial.

[46] Reza Montasari, *Countering Cyberterrorism: The Confluence of Artificial Intelligence, Cyber Forensics, and Digital Policing* (Springer 2024)./ Lorenzo Pupillo and others, *Artificial Intelligence and Cybersecurity: CEPS Task Force Report* (CEPS 2021)./ PW Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (Oxford University Press, 2014)./ Nick Bostrom, *Superintelligence: Paths, Dangers, Strategies* (Oxford University Press, 2017)./ Roman V Yampolskiy, *AI: Unexplainable, Unpredictable, Uncontrollable* (Taylor & Francis Group 2024)./ Chiheb Chebbi, *Mastering Machine Learning for Penetration Testing* (Packt 2018) https://www.packtpub.com/en-gb/product/mastering-machine-learning-for-penetration-testing-9781788997409/chapter/introduction-to-machine-learning-in-pentesting-1/section/artificial-intelligence-and-machine-learning-ch01lvl1sec03 accessed 25 February 2024.

Criteria	Traditional Cyberterrorism	AI-Driven Cyberterrorism
Attack Execution	Cyberattacks conducted by humans	Attacks driven by autonomous AI
Adaptability	Techniques preprogrammed	AI learns, adapts, and evolves in real-time
Disinformation	Content manipulation by hand	Propaganda generated by artificial intelligence & deepfakes
Attribution	Individually traceable	Difficult due to AI autonomy & proxies
Scale & Speed	Slower, requires human intervention	Faster, AI operates autonomously & at scale

Additionally, it may be helpful to analyse the gaps in existing legal frameworks in order to facilitate this process. It is noteworthy that UN Counterterrorism Conventions and UNSC Resolutions focus primarily on physical acts of terrorism, with only a limited emphasis being placed on cyberterrorism powered by artificial intelligence. Therefore, a dedicated international legal instrument would provide a comprehensive framework to combat AI-driven cyber threats. Furthermore, AI-driven cyberterrorism poses a number of unique challenges, including autonomous attacks, advanced evasion techniques, and the difficulty of attribution.

The role of the state is another important consideration. Establish legal accountability for states, private entities, and developers of AI-driven cyber tools that are involved in AI-driven cyberterrorism. It may be possible to ensure compliance with the legal instrument through regular audits and assessments of AI systems used in cybersecurity. Providing training and resources on best practices for AI deployment in cybersecurity to both the public and private sectors may further support compliance efforts.

Additional factors to be considered include the role of technology, and in particular, the behaviour of artificial intelligence. As part of a new legal instrument, international cooperation, regulation of AI technologies with dual-use potential, and attribution mechanisms should also be included. Nevertheless, harmonising legal standards between states is within its reach to facilitate extradition, prosecution, and asset freezing for individuals or groups involved in cyberterrorism. Different legal systems and priorities in various states may pose a challenge to harmonising legal standards globally, resulting in disagreements on definitions and enforcement measures. In addition, some states may be reluctant to cede control over their cyber policies to an international organisation due to concerns regarding their national sovereignty. Additionally, technological advances can outpace the ability of legal frameworks to adapt, making it difficult to maintain regulations that are effective in addressing new threats as they emerge.

Additionally, legal frameworks emphasise human control over AI systems to prevent autonomous attacks. There is no clear liability model for self-learning systems. A potential liability model might involve holding developers responsible for any harm caused by their AI systems, similar to product liability laws. It might also be possible to implement a shared liability model whereby both developers and users are responsible for ensuring the safety and security of AI systems. The establishment of an insurance framework

specifically designed to cover AI-related risks could provide additional protection and encourage responsible AI development.

Transparency is another legal challenge that current legal frameworks have failed to recognise. In AI systems, transparency is crucial as it allows stakeholders to understand how decisions are made and ensure accountability. By making AI processes more transparent, developers can build trust with users and regulators, and it will become easier to identify and correct biases or errors in the system. Furthermore, transparency can facilitate collaboration between different sectors, resulting in better oversight and compliance with legal and ethical requirements.

Due to these challenges, a dedicated international legal instrument is necessary to provide clear legal definitions, regulatory mechanisms, and enforcement provisions tailored to AI-driven cyberterrorism. However, the new legal instrument should strive to address all challenges, such as defining, supply chain risks and categorising AI-driven cyberterrorism.

Criminalisation of AI-driven cyberterrorism under international law

AI is often used to disrupt critical infrastructure or disseminate disinformation to intimidate or coerce governments or societies. International law does not explicitly criminalise AI-driven cyberterrorism, despite its emergence. Under international law, AI-driven cyberterrorism is evolving, but remains fragmented, with recent treaties and frameworks addressing key aspects but leaving significant gaps.

There is no specific mention of AI in most UN conventions, but they cover cybercrimes such as illegal access, system interference, and data misuse, but not terrorism-specific cybercrimes or their use with AI technologies in the Budapest Convention[11]. However, UN resolutions such as 1373 (2001) and 2178 (2014) are focused on preventing terrorist acts and criminalising terrorist financing and recruitment, however, they lack specificity regarding AI-enabled threats and do not guide how to prosecute artificial intelligence-generated disinformation or autonomous attack systems.

Existing legal frameworks regarding the criminalisation of AI-driven cyber terrorism have been examined, and their gaps have been identified. Despite this, it is crucial to develop new legislation that addresses AI-driven threats and their unique challenges. It may be necessary to establish international agreements that facilitate cooperation between states in order to combat cross-border cyberterrorism. Additionally, establishing a task force dedicated to monitoring and updating legal frameworks in response to emerging AI technologies can help ensure that regulations remain effective and relevant.

The challenge of criminalising AI-driven cyberterrorism has been mentioned previously, but the issue of state responsibility is important in regard to this challenge. When AI technologies are used by non-state actors within their jurisdiction, state accountability is not defined by a legal framework. Cyberterrorism driven by artificial intelligence is not adequately criminalised under the current international legal regime. In order to define, prevent, and prosecute such acts under international law, a concerted effort must be made to maintain the delicate balance between security and human rights. Keeping pace with the rapid evolution of AI technology, the international legal framework must also evolve to ensure global safety and accountability. Accordingly, the new legal framework should address all aspects of Al Driven cyber terrorism as well as provide a better and more secure perspective on the issue.

CONCLUSION

A UN-led, comprehensive definition of AI-driven cyberterrorism should be established to guide lawmaking and enforcement. A combination of public and private investments could be used to finance AI-related cybersecurity initiatives. Governments may allocate budgetary resources to advance cybersecurity infrastructure, while private companies may invest in research and development to protect their proprietary technology. It is also possible to establish international collaboration funds through organisations such as the United Nations, in order to pool resources and share the financial burden among a number of states. Nevertheless, it will be beneficial to undo the existing legal framework. In order to criminalise AI-based cyberterrorist acts and clarify state obligations, existing conventions should be amended, or a new treaty should be drafted.

States should provide technical support and training to states that lack the expertise to investigate and respond to AI-enabled threats in international law. Creating regional centres of excellence could serve as a hub for knowledge exchange and skill development tailored to the needs of less experienced states. Furthermore, the formation of international partnerships with leading cybersecurity companies could facilitate technology transfer and provide mentorship programs for local experts. By offering online courses and certification programs in multiple languages, cutting-edge cybersecurity education and resources could be accessed by a wider audience.

There is one main issue that has been raised in other areas of law, which is the balance between security and human rights. In spite of this, there does not exist a comfortable boundary between the two factors. In the case of AI-driven cyberterrorism scenarios, ensure that counterterrorism laws and AI moderation policies (e.g., by tech platforms) do not violate privacy and freedom of expression. AI-driven security measures often involve extensive data collection and surveillance, which can violate an individual's right to privacy. These measures may result in the monitoring of personal communications and online activities, raising concerns about government overreach and the misuse of data. A balance must be struck between security protocols and freedom of expression, as overly aggressive security protocols could undermine public trust in government and technology.

The final point would be to establish an AI-focused intelligence-sharing network (similar to INTERPOL) for tracking threats in real time and coordinating responses. An AI-focused intelligence-sharing network may face obstacles related to data privacy and the protection of sensitive information. The fear of espionage or the misuse of shared data may discourage states from sharing intelligence. Furthermore, the existence of various legal and regulatory frameworks across nations could complicate the establishment of standardised protocols for the exchange of information. In order to ensure that sensitive information is accessible only to authorised individuals, a multi-layered encryption system could be implemented in order to address data privacy concerns. Moreover, establishing a robust framework that includes clear guidelines on the use of data and penalties for data breaches can contribute to building trust among participating states. Transparency and cooperation may be enhanced by establishing a neutral third-party oversight body to monitor compliance and mediate disputes.

In the end, while international law recognises AI-driven cyberterrorism as punishable under adapted cybercrime statutes, gaps in attribution frameworks and dual-use governance still require urgent multilateral action. Lack of international cooperation could result in fragmented approaches to combating AI-driven cyberterrorism, leaving certain regions more vulnerable. Due to this lack of cohesion, laws and standards may also be enforced inconsistently, allowing cybercriminals to exploit legal loopholes and jurisdictional

gaps. Moreover, without coordinated efforts, the global community may not be able to effectively share information and best practices, inhibiting its ability to respond to and mitigate cyber threats.

REFERENCES

- Alexander Blanchard and Jonathan Hall KC, Terrorism and Autonomous Weapon Systems: Future Threat or Science Fiction? (2023) Alan Turing Institute. https://cetas.turing.ac.uk/publications/terrorism-and-autonomous-weapon-systems-future-threat-or-science-fiction
- Ashley Deeks, 'Attribution and the Use of Force in International Law' (2016) 28(1) European Journal of International Law 233.
- Bérénice Boutin, 'State Responsibility in Relation to Military Applications of Artificial Intelligence' (2022) 36(1) Leiden Journal of International Law. https://www.cambridge.org/core/journals/leiden-journal-of-international-law/article/state-responsibility-in-relation-to-military-applications-of-artificial-intelligence/1B0454611EA1F11A8B03A5D2D052C2BE
- C Cath and others, 'Artificial Intelligence and the "Good Society": The US, EU, and UK Approach' (2018) 24(2) Science and Engineering Ethics 505–528. https://link.springer.com/article/10.1007/s11948-017-9901-7
- Carlos Batallas, 'When AI Meets the Laws of War' (2024), IE University. https://www.ie.edu/insights/articles/when-ai-meets-the-laws-of-war/
- Chiheb Chebbi, Mastering Machine Learning for Penetration Testing (Packt 2018). https://www.packtpub.com/en-gb/product/mastering-machine-learning-for-penetration-testing-9781788997409/chapter/introduction-to-machine-learning-in-pentesting-1/section/artificial-intelligence-and-machine-learning-ch01lvl1sec03
- Clementine Swate, Siphesihle Sithungu and Khutso Lebea, An Analysis of Cyberwarfare Attribution Techniques and Challenges (University of Johannesburg 2006).
- Council of Europe, Convention on Cybercrime (Budapest Convention) ETS No 185 (2001).
- CYBLE, 'Harnessing the Power of AI for Real-Time Threat Detection' (2024). https://cyble.com/knowledge-hub/real-time-threat-detection-with-ai/
- Ersin Cahmutoglu, 'The Threat of AI-Driven Cyber Warfare Is Real and It Can Disrupt the World' (2025), TRT World. https://www.trtworld.com/opinion/the-threat-of-ai-driven-cyber-warfare-is-real-and-it-can-disrupt-the-world-18244256
- European Commission, AI Act (2024). https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai
-
- INTERPOL, Cybercrime Global Strategy 2025). https://www.interpol.int/Media/Documents/WPS?limit=12&page=2
- JJ Bryson, ME Diamantis and TD Grant, 'Of, For, and By the People: The Legal Lacuna of Synthetic Persons' (2017) 25(3) Artificial Intelligence and Law 273–291. https://link.springer.com/article/10.1007/s10506-017-9214-9
- Justo Corti Varela and Paolo Davide Farah, Science, Technology, Policy and International Law (Routledge 2024).https://doi.org/10.4324/9781003472421

- Kelley M Sayler, Emerging Military Technologies: Background and Issues for Congress (2024), Congressional Research Service R46458. https://sgp.fas.org/crs/natsec/R46458.pdf
- Kolawole Samuel Adebayo, 'The Answer To AI-Driven Attacks On Critical Infrastructure: Resiliency' (2025) Forbes. https://www.forbes.com/sites/kolawolesamueladebayo/2025/03/25/the-answer-to-ai-driven-attacks-on-critical-infrastructure-resiliency/
- KPMG, Overview of Cybersecurity Law (2017). https://assets.kpmg.com/content/dam/kpmg/cn/pdf/en/2017/02/overview-of-cybersecurity-law.pdf
- Lorenzo Pupillo, Stefano Fantin, Afonso Ferreira and Carolina Polito, Artificial Intelligence and Cybersecurity: CEPS Task Force Report – Technology, Governance and Policy Challenges (Centre for European Policy Studies 2021)
- Lorraine Finlay and Christian Payne, 'The Attribution Problem and Cyber Armed Attacks' (2019) 113 American Journal of International Law. https://www.cambridge.org/core/journals/american-journal-of-international-law/article/attribution-problem-and-cyber-armed-attacks/ADC0F451A9B560D8A070A753E61E874F
- Lucia Stanham, 'AI-Powered Cyberattacks' (2025). https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/ai-powered-cyberattacks/
- Luciano Floridi and Josh Cowls, 'A Unified Framework of Five Principles for AI in Society' (2019) 1 Harvard Data Science Review.
- Mailgun Blog, 'The Golden Age of Scammers: AI-Powered Phishing' (2024). https://www.mailgun.com/blog/email/ai-phishing/
- Michael N Schmitt (ed), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Cambridge University Press 2017).
- Miles Brundage and others, The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation (2018). https://arxiv.org/abs/1802.07228
- Nick Bostrom, Superintelligence: Paths, Dangers, Strategies (Oxford University Press, 2017).
- Osborne Clarke, Cyber Security China (2019). https://www.osborneclarke.com/wp-content/uploads/2019/12/China-Hong-Kong-Cybersecurity-Law-Report-December-2019.pdf
- Plixavra Vogiatzoglou, 'The AI Act National Security Exception' (2024) VerfBlog. https://verfassungsblog.de/the-ai-act-national-security-exception/#:~:text=10.59704/292082becc7cc8e6
- PW Singer and Allan Friedman, Cybersecurity and Cyberwar: What Everyone Needs to Know (Oxford University Press, 2014).
- Richard Bingley, Combatting Cyber Terrorism – A Guide to Understanding the Cyber Threat Landscape and Incident Response Planning (IT Governance Publishing 2024).
- Roman V Yampolskiy, AI: Unexplainable, Unpredictable, Uncontrollable (Taylor & Francis Group 2024).

https://www.taylorfrancis.com/books/mono/10.1201/9781003440260/ai-roman-yampolskiy

- Sangfor Technologies, 'Defining AI Hacking: The Rise of AI Cyber Attacks' (2024). https://www.sangfor.com/blog/cybersecurity/defining-ai-hacking-rise-ai-cyber-attacks
- Securiti, 'What Is China's Cybersecurity Law' (2024). https://securiti.ai/what-is-china-cybersecurity-law/

- Shilpa Mahajan, Mehak Khurana and Vania Vieira Estrela, Applying Artificial Intelligence in Cybersecurity Analytics and Cyber Threat Detection 2024 (John Wiley & Sons Inc.) https://onlinelibrary.wiley.com/doi/book/10.1002/9781394196470
- Tripti Bhushan, 'Artificial Intelligence, Cyberspace and International Law' (2024) 21(2) O.P. Jindal Global Law Review. https://scholarhub.ui.ac.id/cgi/viewcontent.cgi?article=1745&context=ijil
- UN Security Council Resolution 1373 (28 September 2001) UN Doc S/RES/1373.
- UNCCT (United Nations Counter-Terrorism Centre), Algorithms and Terrorism: The Malicious Use of Artificial Intelligence for Terrorist Purposes (2021). https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/malicious-use-of-ai-uncct-unicri-report-hd.pdf
- UNCCT and UNICRI, Algorithms and Terrorism: The Malicious Use of Artificial Intelligence for Terrorist Purposes (2021). https://unicri.it/sites/default/files/2021-06/Malicious%20Use%20of%20AI%20-%20UNCCT-UNICRI%20Report_Web.pdf
- UNESCO (United Nations Educational, Scientific and Cultural Organisation), Recommendation on the Ethics of Artificial Intelligence (2023). https://unesdoc.unesco.org/ark:/48223/pf0000381137
- UNIDIR (United Nations Institute for Disarmament Research), AI and Cybersecurity Workshop: The Challenges of New and Updated Threats (2024). https://unidir.org/event/ai-and-cybersecurity-workshop-the-challenges-of-new-and-updated-threats/
- UNIDIR (United Nations Institute for Disarmament Research), Autonomous Weapon Systems and Cyber Operations (2024). https://unidir.org/files/publication/pdfs/autonomous-weapon-systems-and-cyber-operations-en-690.pdf
- United Nations Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems, Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects (2023). https://docs-library.unoda.org/.../CCW_GGE1_2023_CRP.1_0.pdf
- US Department of Justice, What Is the USA PATRIOT Act?. https://www.justice.gov/archive/ll/what_is_the_patriot_act.pdf